802.11n The Good, The Bad, and The Ugly: Will You Be Ready?

A Whitepaper by AirTight Networks, Inc.

339 N. Bernardo Avenue, Suite 200, Mountain View, CA 94043
www.airtightnetworks.com

Executive summary

IEEE 802.11n, the next generation wireless LAN technology, promises to meet the constant demand for higher data rates, reliable connectivity, and wider coverage. Not a ratified standard yet, 802.11n is creating a lot of buzz with WiFi-certified equipment based on IEEE 802.11n draft 2.0 already in the market. The final standard, expected in mid-2009, will only escalate the adoption of this emerging technology. It is time for businesses to get ready for this inevitable change, whether they invest in pre-standard equipment or wait for the final standard to come out.

802.11n is a big leap in the evolution of wireless LANs. With major advantages in throughput, range and reliability over legacy Wi-Fi protocols, 802.11n opens up new possibilities for running various applications over wireless. The same features that drive these advantages also present technical challenges in network planning, installation, security, and operation of these networks. The numerous ways in which 802.11n choices can impact legacy 802.11a/b/g networks cannot be ignored. Enterprises should carefully consider these aspects to maximize the business benefits from 802.11n.

Introduction

In theory, the significant performance gains from 802.11n over its predecessors 802.11a and 802.11g are clear. But in practice, achieving those gains is not just plug-and-play. The extent to which 802.11n can deliver on its promises in real life depends on many factors: the configuration and placement of your 802.11n equipment, 802.11n-readiness of your network infrastructure and wireless security, and how well you manage the surrounding RF environment.

802.11n from 30,000 feet

802.11n brings many new features to deliver longer range and a more than ten-fold increase in the data rates as compared to legacy 802.11 protocols. Foremost is the ability of 802.11n to transmit and receive simultaneously over multiple antennas, commonly known as MIMO (multiple inputs multiple outputs). MIMO can be exploited to transfer multiple unique data streams to pump more bits in the same time and achieve higher data rates. This MIMO technique is commonly known as spatial multiplexing. Or MIMO can be used for transmitting and receiving copies of the same data stream over multiple antennas to increase the range. This MIMO technique is commonly known as spatial diversity. The data rate can be more than doubled by efficiently bonding two 20 MHz channels into one 40 MHz channel.

802.11n defines a total of 77 modulation and coding schemes (MCS) of which 16 (MCS 0-15) are mandatory. Depending on the MCS, the channel width, and the guard interval—that determines how tightly the data carrying symbols are packed, 802.11n can achieve data rates up to 600 Mbps. Most vendors today support the mandatory MCS 0-15 with data rates up to 300 Mbps.

Because of inefficiencies inherent to 802.11 protocols, simply increasing the data rate does not result in the same order of improvement in throughput for applications. To improve the bandwidth efficiency, and hence the maximum achievable throughput, the 802.11n draft standard proposes frame aggregation and block acknowledgement (Block ACK). Instead of sending a single data unit (MSDU) per 802.11 frame (MPDU), multiple packets can be aggregated (A-MSDU) in a single frame or multiple frames can be aggregated into a larger frame (A-MPDU) before transmission. Unlike legacy 802.11 protocols where the receiver acknowledges every successfully received frame, 802.11n allows a receiver to cumulatively acknowledge multiple frames using a Block ACK. In short, these techniques improve the efficiency of data transmission, translating into higher throughput for applications.

Migrating to 802.11n

Coexistence with legacy WLANs

The IEEE 802.11n standard defines a high throughput (HT) mixed mode that is backwardcompatible with legacy 802.11a/b/g devices. An 802.11n AP in this mode enables high data rates for 802.11n clients while supporting legacy clients. But backward compatibility comes at the cost of increased overhead; the effect is similar to when 802.11g was designed to be backward compatible with 802.11b.

Clients operating at legacy data rates can additionally limit the maximum capacity of an802.11n AP. 802.11a/b/g devices will occupy the medium much longer than faster 802.11n devices for transmitting the same amount of data. With large proportion of 802.11a/b/g clients, the throughput gains due to 802.11n can become negligible. One way enterprises can avoid this problem is by using 802.11n APs with dual band radios-one radio is used by legacy clients, while the other is dedicated for 802.11n clients. If this is not feasible, then enterprises should at least disallow connections at very low data rates (e.g., 1, 2, 5.5, 6 Mbps) and plan their WLAN coverage accordingly. Organizations deploying a fresh WLAN could also consider using 802.11n APs with the optional 802.11n "Greenfield" mode that is not backward compatible and is expected to deliver best performance.

End-to-end 802.11n upgrade

To get full benefits of 802.11n, many businesses will gradually replace their legacy APs as well as clients with 802.11n devices. But this alone will not guarantee peak 802.11n performance. Upgrading the backhaul infrastructure is equally important to ensure that it does not become the bottleneck. Below are three issues that enterprises will need to consider.

Power requirements

With dual radios and three MIMO antennas per radio, the typical power consumption (~18 W) of a full-capacity 802.11n AP is more than the 12.95 W the 802.3af PoE standard can handle. The 802.3at standard when available will be able to support the higher power required by 802.11n APs. Most 802.11n APs can nevertheless be run on 802.3af at a reduced capacity (e.g., using two antennas instead of three). Some vendors are offering proprietary solutions that support enough power for running their 802.11n APs on full capacity on existing PoE switches.

Gigabit Ethernet

The 10/100 Mbps Ethernet is the prevalent LAN technology. Today most 802.11n APs can deliver close to 150 Mbps peak throughput in the mixed mode. This throughput will grow in the future as vendors start implementing performance-enhancing optional features into their equipment. Upgrade your wired LAN to Gigabit Ethernet to sustain the 100+ Mbps high throughput if you expect heavy wireless usage.

Impact on WLAN controllers

In most centralized WLAN architectures, all control and data traffic to and from the APs is tunneled through a central WLAN controller. Legacy WLAN controllers are unlikely to be able to handle the manifold increase in the traffic flow from multiple 802.11n APs. Enterprises will have to choose between supporting lesser number of 802.11n APs per legacy WLAN controller and doing a forklift upgrade of their controllers.

Predictive Planning

Careful RF planning is a pre-requisite for a successful 802.11n rollout. 802.11n exhibits RF characteristics that are very different from traditional WLANs. 802.11n leverages MIMO to exploit multipath fading and improve the RF coverage in unexpected ways. The wider coverage and the use of wider 40 MHz channels increase the likelihood of interference. Simply swapping existing APs for 802.11n APs may not be necessary and can even be detrimental. The effect of the various RF factors and coexistence with legacy devices needs to accounted for when planning for capacity of your 802.11n WLAN.

Use a WLAN RF planner that supports important 802.11n features such as MIMO, 20 and 40 MHz channels, and frame aggregation. Make sure the planning tool allows you to model your environment with ease, gives you the choice to plan for coverage and capacity, suggests AP placement and channel assignment, and lets you quickly simulate "what-if" scenarios for comparing different 802.11n migration plans. Ability to do a site survey integrated into a WLAN planning tool can be handy. For instance, the tool could account for neighboring APs in your environment and calculate their impact in terms of interference and help fine tune settings on your APs. Or the tool could be used to calibrate and better predict the 802.11n coverage based on real-life measurements on site.

Securing Your 802.11n Investment

Higher density of wireless vulnerabilities

802.11n will amplify existing wireless vulnerabilities in a network by exposing them over greater distances. Before the advent of 802.11n, if a wireless backdoor in your network was like having an unattended Ethernet port in your parking lot; 802.11n will extend that backdoor few blocks down from your parking lot. In other words, the density of wireless vulnerabilities will increase as the density of wireless LANs increases in the post-802.11n world.

Upgrade your WIPS

Enterprises planning migration of their WLAN infrastructure to 802.11n need to upgrade their security for comprehensive protection from all types of 802.11n rogue devices and unauthorized connections. A legacy wireless intrusion prevention system (802.11a/b/g WIPS) can detect existence of 802.11n devices operating in legacy or HT mixed mode. But it cannot detect new threats stemming from 802.11n:

- Client associations at 802.11n data rates -- Your 802.11n clients connecting to external 802.11n APs or unauthorized 802.11n clients connecting to 802.11n rogue APs or your 802.11n APs will go undetected.
- New 802.11n-specific attacks -- Certain unprotected management frames related to Block ACKs can be exploited to launch a denial-of-service (DoS) attack on an 802.11n network.
- Greenfield mode -- In future, vendors will start shipping equipment with this optional 802.11n mode that can be detected only by WIPS with full 802.11n support.

Selecting the right security solution

Careful selection of your WIPS solution is even more important with 802.11n. Businesses should be aware of the risks they face from WIPS solutions which are created from wired side testing methodology, are cobbled together as an add-on to WLAN infrastructure or are based on handheld wireless security solutions.

A side-effect of 802.11n that will expose and overwhelm inaccurate and poorly implemented WIPS is the significant increase in the number of false alarms. The increase in WLAN density means WIPS without accurate auto-classification will leave you stressed with more devices to worry about and manually classify as authorized, unauthorized, rogues, and external devices. Handheld based site surveys for wireless vulnerability assessment and security audits will not scale with large Wi-Fi footprints and provide only a moment in time without true visibility into your ongoing security posture.

Accurate location tracking is an important component of a WIPS as it allows you to quickly locate and remove malicious or anomalous devices. MIMO effects in 802.11n will fool naïve, RSSI-based location tracking in a mixed deployment of legacy and 802.11n sensors causing more errors.

Performance Monitoring

With 802.11n, more and more enterprises will rely on their WLAN for running business critical applications; reliability and uptime on par with wired networks will be expected. Meeting these expectations is non-trivial as wireless is a shared medium, and the performance of a WLAN heavily depends on its RF environment, including your neighbors' wireless devices.

The RF environment in which your WLAN resides will become more dense and dynamic with 802.11n. Compared to legacy devices, an 802.11n device will typically see more Wi-Fi devices around it because of its ability to decode signals over a longer distance. More the devices seen, greater the likelihood of interference from neighboring Wi-Fi networks. Use of 40 MHz channels will exacerbate this problem, especially in the already crowded 2.4 GHz frequency band. Another challenge 802.11n clients face is the disproportionate drop in their throughput caused by legacy (802.11a/b/g) clients sharing the bandwidth.

These anomalies can leave your 802.11n network crippled with sub-optimal bandwidth utilization, poor quality of service for applications, and inconsistent experience for the end-users. To avoid getting overwhelmed by complaints from dissatisfied end-users, it is prudent for network administrators to proactively have an 802.11n-ready WLAN monitoring system in place. This is especially important if you anticipate mixed (legacy + 802.11n) deployments and a dense Wi-Fi neighborhood. Conduct a performance audit periodically for analyzing if your 802.11n network is healthy and consistently performing close to its peak capacity, and for troubleshooting if a problem is diagnosed.

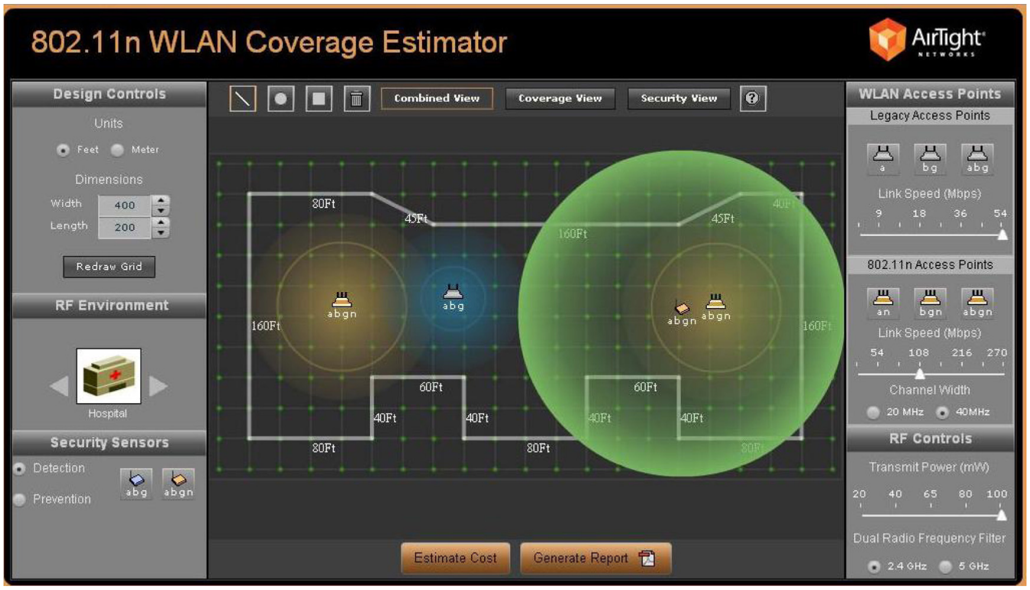
Plug and Play Your 802.11n with AirTight Networks

AirTight Networks offers a suite of solutions and services for seamlessly planning, monitoring, and securing your 802.11n investment. The goal is to enable enterprises to reap the benefits of 802.11n without getting bogged down by the challenges.

802.11n planning made easy

Free , Web-based WLAN planning

AirTight Networks' WLAN Cost Estimator (WCE) is the first-of-its-kind free, online tool for high-level planning of your WLAN rollout, including 802.11n. WCE does not replace a full-fledged Wi-Fi Planner, but it is useful to get a rough estimate of the number of access points (legacy vs. 802.11n) required to meet your coverage goals and the number of wireless scanners needed to detect and prevent wireless threats, and to quickly evaluate the total projected cost for your WLAN deployment.



Units ● Feet ○ Meter

Dimensions

Width 400

Length 200

● Detection

○ Prevention

Channel Width ○ 20 MHz ● 40MHz

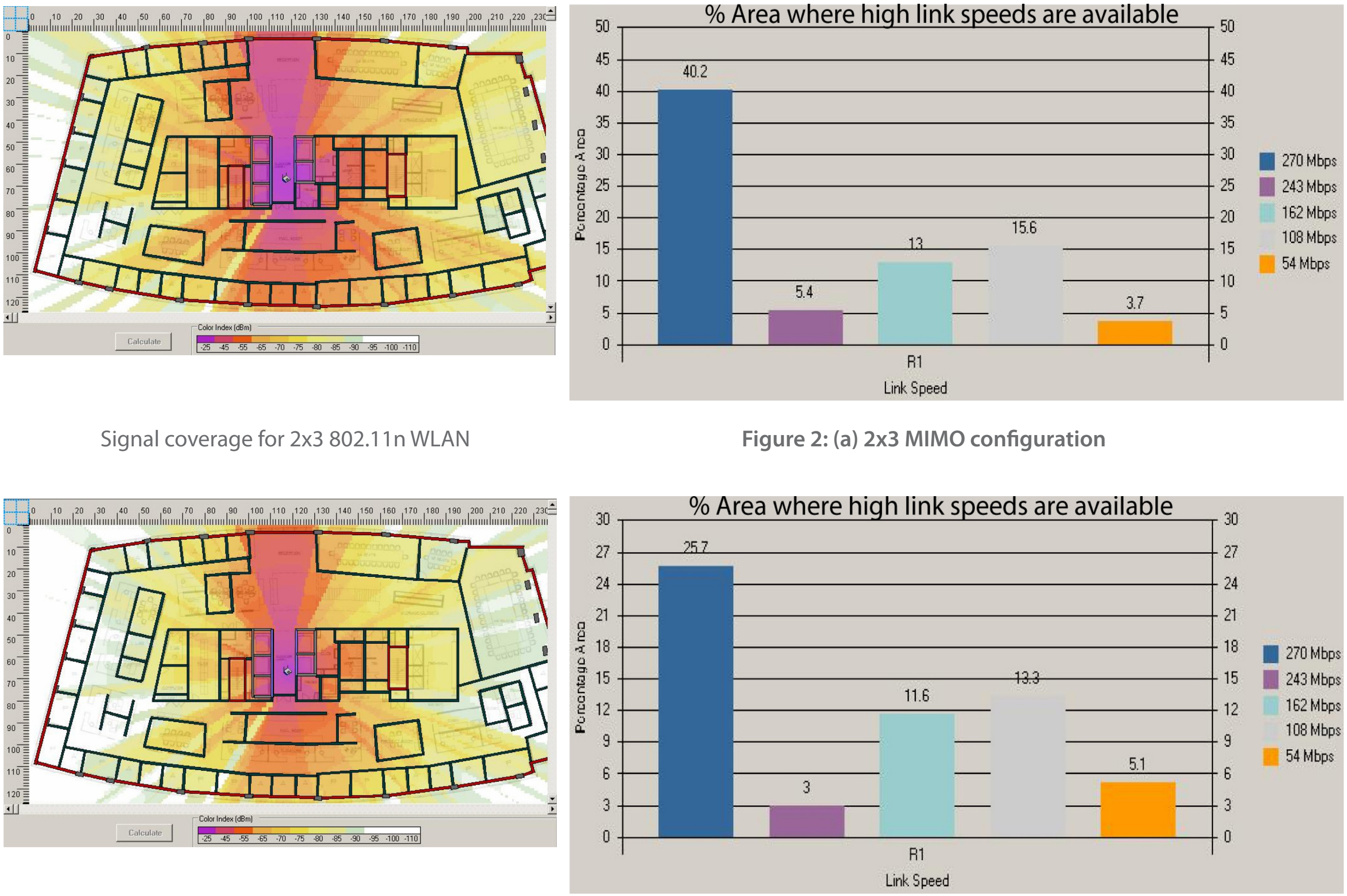
Dual Radio Frequency Filter ● 2.4 GHz ○ 5 GHz

Figure 1: WLAN Coverage Estimator

SpectraGuard® Planner

For a thorough planning of your WLAN coverage, capacity, and security, AirTight Networks' SpectraGuard® Planner is recommended. It models all 802.11n features currently available in the market: 2x2, 2x3, and 3x3 MIMO, 20 and 40 MHz channels, up to 300 Mbps link speeds, and guard interval of 400 and 800 ns. It allows you to quickly configure, play with, and compare different 802.11n scenarios enabling you to make the best choice — whether it is a new 802.11n deployment or migration of your legacy infrastructure to 802.11n. You can take advantage of the same benefits for planning 802.11n security coverage.

Sample screenshots from SpectraGuard® Planner, illustrating the signal coverage and corresponding link speed distribution of an 802.11n AP for 2x2 and 2x3 configurations, are shown in Figure 2.



Signal coverage for 2x3 802.11n WLAN

Figure 2: (a) 2x3 MIMO configuration

Signal coverage for 2x2 802.11n WLAN

Figure 2: (b) 2x2 MIMO configuration

Figure 2: Estimated 802.11n AP coverage in SpectraGuard® Planner

In addition to full 802.11n support, other highlights of SpectraGuard® Planner are the ability to import your floor plan as an AutoCAD or image file, user-friendly controls to effortlessly define your environment, a comprehensive list of the latest Wi-Fi access point models to choose from, WLAN capacity and coverage planning wizard, automatic calculation and placement of access points, integrated site surveyor for calibration, and rich views (e.g., based on signal strength, interference, link speed) to gain visibility into estimated Wi-Fi connectivity and security coverage.

You can also take advantage of AirTight's expert WLAN Planning Services to receive detailed guidance on the best way forward to migrate your WLAN infrastructure to 802.11n, and how you could secure it using AirTight's 802.11n-ready wireless intrusion prevention.

Industry's best wireless protection

802.11n presents an inflection point for the concentration of wireless vulnerabilities and threats, raising the bar for enterprise wireless security. Automation and accuracy are the keywords for selecting an 802.11n-ready wireless security solution.

AirTight Networks' SpectraGuard® wireless intrusion prevention system (WIPS) is the industry's first 802.11n-ready WIPS. Its salient features are:

- State-of-the-art 802.11n MIMO wireless scanner (shown in Figure 3) that is dual-radio (2.4 GHz and 5 GHz), backward compatible, and can operate at full capacity on existing 802.3af PoE
- Comprehensive protection against 802.11n threats with industry's only complete end-to-end wireless vulnerability management service
- Patented accurate auto-classification of wireless devices
- Minimal false positives and false negatives
- Patented automatic over-the-air intrusion prevention against multiple threats simultaneously
- Accurate location tracking, even in mixed (legacy + 802.11n) deployments
- Rich, executive style reports for assessment of your organization's wireless security posture including regulatory compliance

Figure 3: AirTight's 802.11n dual-radio MIMO wireless scanner

Business benefits

"Lean back" wireless security

With 802.11n, enterprises will see a significant rise in the number of unauthorized devices and activities in their airspace. This will expose poorly implemented, noisy WIPS and other security solutions — network security administrators will have to spend more hours sifting through the barrage of false alerts generated by these "lean forward" systems. AirTight's proven accurate, automated classification of newly discovered wireless devices and automatic blocking of wireless threats makes it the only "lean back" wireless security product.

Reduced TCO

AirTight can reduce your total cost of ownership (TCO) with reduced WIPS scanner density by up to 30%. AirTight's 802.11n wireless scanner leverages MIMO for expanding its threat detection coverage as compared to an 802.11a/b/g scanner. This will reduce the number of scanners, and hence the time and the cost required for installation. SpectraGuard® supports integration with Cisco's WLC — which means your Cisco WLAN infrastructure can be repurposed for accurate location tracking, further reducing your costs. The online WLAN Cost Estimator (WCE) lets you do high-level WLAN planning and estimate costs for free.

Maximize ROI

Careful planning of your 802.11n investment—WLAN infrastructure and WIPS—using SpectraGuard® Planner will give you an optimal baseline to begin with to meet your capacity and coverage goals. It will avoid overprovisioning and expensive revisions of your WLAN layout. Your WIPS investment is future-proof as AirTight's 802.11n wireless scanner can be upgraded to conform with the 802.11n standard when it is ratified. The scanner is compliant with the 802.3af PoE, which means no upgrade of your existing PoE infrastructure is necessary.

Conclusions

802.11n is poised to become the de facto wireless LAN technology in the near future. Four key factors that underpin successful 802.11n execution are: a sound migration strategy, RF planning, up-to-date wireless security, and performance monitoring. Understanding these aspects will help businesses avoid expensive mistakes and reap maximum benefits from their 802.11n investment. AirTight Networks is uniquely positioned for helping organizations make a seamless transition to 802.11n — with industry's best wireless security, reduced TCO, and maximum ROI.

About AirTight Networks

AirTight Networks is the global leader in wireless intrusion prevention solutions offering customers best-of-breed technology to automatically detect, classify, locate and block all current and emerging wireless threats. AirTight's award-winning products are used by customers globally in the financial, government, retail, manufacturing, transportation, education, healthcare, telecom, and technology industries. AirTight owns the seminal patents for wireless intrusion prevention technology with 11 U.S. patents and two international patents granted (UK and Australia), and more than 25 additional patents pending. AirTight Networks is a privately held company based in Mountain View, CA. For more information please visit www.airtightnetworks.com

AirTight Networks and the AirTight Networks logo are trademarks; AirTight and SpectraGuard are registered trademarks of AirTight Networks, Inc. All other trademarks are the property of their respective owners.